بسم الله الرحمن الرحيم

بسم الله والحمد لله والصلاة والسلام على محمد بن عبد الله المجاهد الذي قال –وعليه أفضل الصلوات وأتم التسليم-: "أنا نبي الرحمة، ونبي الملحمة".

وبعد إن شاء الله هذه الحلقة الأولى من دورة (أمنيات التشفير للذئب).

نبذة

أعلم يا كريم أن علم التشفير الحديث هو بناء على علم التعمة القديم الذي أخترعه أجدادانا من أهل الإسلام ومنهم : يعقوب بن إسحاق الكندي رحمه الله تعالى الذي ألف (رسالة الكندي في استخراج المعمى) وهي مخطوطة مكتشفة منذ فترة قريبة.

وفي هذا الكورس إن شاء الله سنتعامل مع التشفير الحديث الذي يعتمد على المبادئ المتطورة حتى نقدر أن ندمجها بالنهاية مع أحد الوسائل التكنولوجية المعاصرة.

اهم المصطلحات

1- **الخوارزمية :** هي مجموعة من الخطوات الرياضية والمنطقية والمتسلسلة اللازمة لحل مشكلة ما وهي من صنع جدنا الخوارزمي وهي أساس بناء كل التكنولوجيا المعاصرة.

2- **ف (المفتاح) :** هو الأداة التي أدخلها على النص لكي أكشف تعمية أو أعمّي بها كما الحال مع مفتاح المنزل فمن خلاله أستطيع أن اغلق المنزل فلا يتطلع على ما بداخله أحد بالخارج واستطيع أن افتحه.

3- **ش (المشفر) :** هو النص النهائي المُعمى.

4- **ص(الأصلي) :** هو النص الأصلي قبل التعمية أو بعد كشف التعمية.

5- **ع (المفتاح العام) :** يشرح في حين الوصول له إن شاء الله.

6- **خ (المفتاح الخاص) :** يشرح في حين الوصول له إن شاء الله.

7- **بق (باقي القسمة):** وهو الرمز mod في الالة الحاسبة .

وما سبق الحديث عنه مهم للغاية في كل الدروس القادمة إن شاء الله وفقك الله أخي لما يحبه ويرضاه وجعلك سيفاً على أعداء الدين ويد عون لإخوانك المسلمين.

الدرس الأول (خوارزمية قيصر)

بسم ربي الأعلى وبعد في هذا الدرس إن شاء الله سندرس الخوارزمية الأولى من خورزميات التعمية الحديثة ألا وهي خورزمية القصير ومفادها التالي...

الحروف(28 حرف ويبدأ العد من صفر)

ي	و	هـ	ن	م	ل	ك	ق	ف	غ	ع	ظ	ط	ض	ص	ش	س	ز	ر	ذ	د	خ	ح	ج	ث	ت	ب	أ
27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

قاعدة التعمية

الحالة الأولى أن (ص+ ف) ليس أكبر من 27 فايصير القانون كالأتي

ش = (ص + ف)

الحالة الثانية أن (ص+ ف) أكبر من 27 فايصير القانون كالأتي لإعادة الرقم الى مسراه ال برقم داخل ال 28 حرف

ش = (ص + ف) بق28
ويحسب(بق28) بالشكل التالي
لو قلنا أن الناتج من جمع (ص + ف) = 30
إذا "30-30 ÷ 28X28" = 2
او
بالبدأ من الأول وهو الأفضل
أي إذا كان المفتاح مثلا 3 ورقم الحرف 27
فالحل إذا أن بعد ال27 يبدأ يعد من الصفر بالمفتاح(3)حتى يصل الى 2 وهو الحرف المُعمى

مثال

مطلوب تعمية نص "السلام على من أتبع الهدى" بمفتاح (3)

الحل

أولاً التعمية

الحرف الأصلي	التعمية	الحرف المُشَفَّر	الناتج
أ	3 = 3+ 0	ت	-
ل	25 = 3 + 22	هـ	-
س	14 = 3 + 11	ض	-
ل	25 + 3 + 22	هـ	-
ا	3 = 3 + 0	ت	-
م	26 = 3 + 23	و	-
			تهضهتو
ع	20 = 3 + 17	ق	
ل	26 = 3 + 22	و	
ي	30 = 3 + 27 ومن ثم هنا وجدنا أن الرقم 30 تعدى الأرقام المتاحة فنتجه للحالة الثانية وهو إداخلها في (بق28) او	ت	

		(mod28) وفيكون الناتج كالتالي إختصاراً: 2 = 28 % 30 تفصيلاً: 30-30 (ناتج "ف+ص") ÷ 28X28 (عدد حروف اللغة العربية) 2 =	
قوت			
	و	26 = 3 + 23	م
	ي	27 = 3 + 24	ن
وي			
	ث	3 = 3 + 0	ا
	ح	5 = 3 + 2	ت
	ج	4 = 3 + 1	ب
	ق	20 = 3 + 17	ع
ثحجق			
	ث	3 = 3 + 0	ا
	هـ	25 = 3 + 22	ل
	أ	= 3 + 25 28 بق28 0 =	هـ
	ز	10 = 3 + 7	د
	ت	= 3 + 27 30 بق28 2 =	ى
ثهأزت			

قاعدة كشف التعمية

ص = (ش - ف)
وفي حالة خروج رقم بالسالب يُعد من رقم 27 حتى يصل لنهاية المفتاح تنازلياً.

مطلوب تعمية نص " تهضهتو قوت وي ثحجق ثهأزت" بمفتاح (3)

الحل

الحرف الأصلي	التعمية	الحرف المُشَفّر	الناتج
ت	3 - 3 = 0	أ	-
هـ	25 - 3 = 22	ل	-
ض	14 - 3 = 11	س	-
هـ	25 - 3 = 22	ل	-
ت	3 - 3 = 0	ا	-
و	26 - 3 = 23	م	-
			السلام

ويُترك لك أخي كشف تعمية باقي النصوص التي بالمثال ولنا لقاء في الدرس القادم إن شاء الله..وفقك الله لكل خير يا ذنب الإسلام.

بقلم
أبو حمزة الحنفي